Release Notes

McAfee VirusScan Enterprise 8.8.0 Patch 4 Software

About this release

Thank you for using this McAfee product. This document contains important information about the current release. We strongly recommend that you read the entire document.

Purpose

This release of McAfee® VirusScan® Enterprise 8.8.0 contains a variety of improvements and fixes.

Although McAfee has thoroughly tested this release, we strongly recommend that you verify this update in test and pilot groups prior to mass deployment. Review the *New features*, *Resolved issues*, and *Known issues* sections for additional information.

Important Patch 4 is the last release of VirusScan Enterprise 8.8 to support Windows 2000.

For a list of supported environments and latest information for VirusScan Enterprise 8.8.0 on Microsoft Windows, see KnowledgeBase article KB51111.

Patch version

- **Patch 4** package — Updates VirusScan Enterprise 8.8.0 clients, **with Patch 1 (32-bit) or Patch 2 (64-bit) only**.

Important This package does not upgrade VirusScan Enterprise version 8.8.0.777 (RTW).

To update with the **Patch 4** package:

- On 64-bit systems, first install Patch 2, then Patch 4.
- On 32-bit systems, first install Patch 1, then Patch 4.

Alternatively, uninstall VirusScan Enterprise 8.8.0 and reinstall with the **Repost**

Patch 4 package.

- **Repost Patch 4** package for Windows — Includes full installation for new systems or VirusScan Enterprise 8.7i systems.
- Both the Patch and Repost packages include management packages for ePolicy Orchestrator:
  - **Patch Extension** for VirusScan Enterprise VIRUSCAN8800(368).zip
  - **Patch Reports** for VirusScan Enterprise VIRUSCANREPORTS120(236).zip

Refer to KnowledgeBase article KB51111 for the most current VirusScan Enterprise 8.8.0 details.

Build date
January 15, 2014

Rating
Critical — McAfee rates this release as critical for all environments to avoid a severe business impact. This update should be applied as soon as possible.

For more information about patch ratings, see McAfee KnowledgeBase article KB51560.

New features

This release of the product includes these new features for all supported operating systems.

Hotfix installation report
This release includes a new property in the ePolicy Orchestrator Query Builder to report on Hotfixes that are installed on VirusScan Enterprise client systems.

Feature Group	Result Type	Property (Column)
System Management	Managed Systems	VirusScan Enterprise – Additional Properties | VSE HotFixes

To run an ePolicy Orchestrator report that lists the Hotfixes that have been installed on VirusScan Enterprise client systems:

1. In ePolicy Orchestrator, select Queries & Reports.
2. Click the Query tab, then click New.
3. Select System Management from the Feature Group and Managed Systems from the Result Types, then click Next.
4. Specify the Chart options, then click Next.
5. From Available Columns, select VirusScan Enterprise – Additional Properties | VSE HotFixes, then click Next.
6. Specify the Filter options, then click Run.

Important To search for a specific Hotfix, in the Filter tab, use the Contains comparison to filter for the Hotfix number in the Value field.

For information on queries and reports, see the ePolicy Orchestrator Help.

Access Protection and On-Access Scan status report
This release includes the ability to report the status of Access Protection and On-Access Scan on VirusScan Enterprise client systems:

- New predefined queries in ePolicy Orchestrator under Queries & Reports:
  - VSE: Access Protection Enabled Status
  - VSE: On-Access Scanner Enabled Status
-

New properties in the ePolicy Orchestrator Query Builder.

Feature Group	Result Type	Property (Column)
System Management	Managed Systems	VirusScan Enterprise - Additional Properties | AP Enabled State VirusScan Enterprise - Additional Properties | OAS Enabled State

To run an ePolicy Orchestrator report that lists the Access Protection and On-Access Scan status on VirusScan Enterprise client systems:

1. In ePolicy Orchestrator, select Queries & Reports.
2. Click the Query tab, then click New.
3. Select System Management from the Feature Group and Managed Systems from the Result Types, then click Next.
4. Specify the Chart options, then click Next.
5. From Available Columns, select AP Enabled State and OAS Enabled State from VirusScan Enterprise - Additional Properties, then click Next.
6. Specify the Filter options, then click Run.

For information on queries and reports, see the ePolicy Orchestrator Help.

VirusScan Enterprise properties moved in the Query Builder

In this release, several properties in the ePolicy Orchestrator Query Builder moved to a different feature group (in the Result Type tab.

Property	Previous Feature Group	New Feature Group
Machine Type	Others	System Management
On-Access Scan Artemis Level		
On-Demand Scan Artemis Level		
Email Scan Artemis Level		

To run an ePolicy Orchestrator report using these properties on VirusScan Enterprise client systems:

1. In ePolicy Orchestrator, select Queries & Reports.
2. Click the Query tab, then click New.
3. Select System Management from the Feature Group and Managed Systems from the Result Types, then click Next.
4. Specify the Chart options, then click Next.
5. From Available Columns, select the properties from VirusScan Enterprise - Additional Properties, then click Next.
6. Specify the Filter options, then click Run.

For information on queries and reports, see the ePolicy Orchestrator Help.

Access Protection process inclusion and exclusion limits and behavior

In this release, when creating Access Protection rules in ePolicy Orchestrator, VirusScan Enterprise now:

- Expands Processes to include and Processes to exclude fields to a maximum of 5199 characters.

- Warns when the number of characters in the field is within 200 characters of the maximum character limit.
- Prevents these fields from exceeding the maximum character limit.

ScriptScan browser support

ScriptScan now supports:

- Internet Explorer 10
- Internet Explorer 11

Note With Internet Explorer 11, Enhanced Protection Mode (EPM) might display an erroneous error message that ScriptProxy is disabled. However, ScriptScan is still scanning. To investigate ScriptScan performance issues, you must disable EPM.

Note ScriptScan does not support Mozilla Firefox browsers. Firefox blocks the ScriptScan DLLs from loading.

Updated components

This release includes updated versions of the following components.

Component	Version	Notes
Engine	5600	
McAfee Agent	4.8.0.887	
VSCore	15.1	This version of VSCore allows VirusScan Enterprise to install on systems with expired certificates.
VSCAN.BOF	659	

New features — Windows 8 and Server 2012 systems

This release includes support for Windows 8.1 (Blue) and Server 2012 R2 systems.

Note Patch 3 included additional features for supported Windows systems.

New features — other supported Windows systems

This release includes these new features for supported Windows systems other than Windows 8 and Server 2012.

Note These features were supported in Patch 3 for Windows 8 and Server 2012 systems only.

Connected standby mode

This release of VirusScan Enterprise provides support for systems in connected standby mode (also called *Always On Always Connected* or AOAC).

Note AOAC mode is only supported on Windows 8 systems with hardware chips that support AOAC.

- **AOAC suspended mode**

  When the system is in AOAC suspended mode, VirusScan Enterprise does not perform scans or DAT updates. If an on-demand scan (ODS) starts before the system hibernates in AOAC or battery mode, the ODS pauses. If Run missed tasks

option is selected, any missed ODS scans run immediately when the system wakes from suspended mode.

- **User present mode**

  When a user is present (keyboard and/or mouse interaction within 5 minutes), VirusScan Enterprise performs any on-demand scans and DAT updates as specified by the schedule.

Policy settings changes

New or changed setting	Console option	Extension option
Cookie scans have been removed.	Scan cookie files on the On-Access Scan Properties | General Settings | General tab	Scan cookie files on the On-Access General Policies | General tab
Artemis (GTI) sensitivity level is now set to Medium by default for new installations only (not upgrades). **Note** Policy settings in McAfee ePO override this default.	Sensitivity level on the On-Access Scan Properties | General Settings | General tab	Sensitivity level on the On-Access General Policies | General tab
VirusScan Enterprise Console now includes a menu option that links to KnowledgeBase article KB65944.	Help | Known Issues	n/a
Buffer Overflow Protection has been removed from Windows 8 and Windows Server 2012.	Buffer Overflow Protection in the Task list	Buffer Overflow Protection Policies

Client task settings changes

New or changed setting	Console option	Extension option
Cookie scans have been removed.	Scan cookie files on the On-Demand Scan Properties | Scan Locations tab	Scan cookie files on the On-Demand Scan Client Task | Scan Locations tab
Artemis (GTI) sensitivity level is now set to Medium by default for new installations only (not upgrades). **Note** Client task settings in McAfee ePO override this default.	Sensitivity level on the On-Demand Scan Properties | Performance tab	Sensitivity level on the On-Demand Scan Client Task | Performance tab

Registry settings changes

New or changed setting	Registry entries	DWORD default value

Delayed Write Scan mode is now enabled by default.
 	
This mode delays all scans of modified files to lower priority background threads. This improves performance for processes that write data to disk frequently and/or write a lot of data in a short amount of time.
 	
Important To maintain security, you must enable the **Scan on Read** setting.
 	
Removable media and network file share write operations are still scanned immediately on **Close**.
 	
For more information, see KnowledgeBase article KB75374.
	• 32-bit systems: HKLM\Software\McAfee\SystemCore\VSCore\On Access Scanner\McShield\Configuration:
	  ◦ **DelayAllWriteScans**
	  ◦ **BackGroundAllDelayedScans**
	• 64-bit systems:
	HKLM\SOFTWARE\Wow6432Node\McAfee\SystemCore\VSCore\On Access Scanner\McShield\Configuration:
	  ◦ **DelayAllWriteScans**
	  ◦ **BackGroundAllDelayedScans**
		1 (enabled)

On-Demand Scanner is now limited to one thread per CPU, 6 threads total by default. This limits the amount of memory used by ODS.
 	
• To activate this feature, the System utilization slider setting (on the On-Demand Scan Properties, Performance tab) must be set to Below Normal.
• To change the maximum number of threads, set the DWORD value.
• To deactivate this feature, set the DWORD value to "0".
	• 32-bit systems: HKLM\SOFTWARE\McAfee\DesktopProtection\Tasks:
	  ◦ **dwUserDefinedMaxThreads**
	• 64-bit systems:
	HKLM\SOFTWARE\Wow6432Node\McAfee\DesktopProtection\Tasks:
	  ◦ **dwUserDefinedMaxThreads**
		6 (maximum number of threads)

Artemis performance is increased when scanning large files.
 	
Large files are now hashed and, in parallel with the scan, an Artemis query runs to determine whether the file is known to be clean. If so, the scan stops.
 	
Note The Artemis query runs regardless of the sensitivity level.
 	
Because hashes are cached, future scans can use the existing hash if the file hasn't been modified.
 	
By default, files larger than 5MB
	• 32-bit systems: HKLM\SOFTWARE\McAfee\SystemCore\VSCore:
	  ◦ **PreScanSizeKBForArtemisScan**
	• 64-bit systems:
	HKLM\SOFTWARE\Wow6432Node\McAfee\SystemCore\VSCore:
	  ◦ **PreScanSizeKBForArtemisScan**
		5000

are hashed. To specify the size of files that trigger this behavior, set the DWORD value.

ASLR and DEP features

This release of VirusScan Enterprise enables the following security features for all VirusScan Enterprise components:

- Address Space Layout Randomization (ASLR)
- Data Execution Prevention (DEP)

Resolved issues

Here is a list of issues from previous releases of the software that have been fixed.

Issues resolved in this release

These issues were resolved in the VirusScan Enterprise Patch 4 release.

1 **Issue** — McTray.exe stopped working when logging off or during upgrades. (Reference: 753122)

Resolution — Fixed a timing issue in the VirusScan Enterprise plug-in.

2 **Issue** — Windows Server 2008 Server systems did not delete session when users logged out, so system resources continue to be consumed by inactive sessions. (Reference: 778101)

Resolution — Revised the mfehidk.sys driver to eliminate a dependence on resources that might not be freed when a user logs out.

3 **Issue** — Margin settings are altered (reset) when viewing settings on localized Outlook version on English operating system. (Reference: 782155)

Resolution — VirusScan Enterprise Outlook Email scanner now writes registry data using installed locale instead of the user locale format.

4 **Issue** — Command-line On-Demand Scans ignored the /logformat switch, and instead wrote logs in the default format (UTF-8). (Reference: 786061)

Resolution — The /logformat settings are now used and scan logs are written in proper format.

5 **Issue** — Bugchecks could occur in mfehidk.sys. (Reference: 797573, 795174)

Resolution — Modified mfehidk.sys to ensure that context data is passed between pre-operation and post-operation handlers in a manner that doesn't cause invalid memory references.

6 **Issue** — ePolicy Orchestrator administrators could not reliably determine the status of the On-Access Scans on client systems. (Reference: 820636)

Resolution — VirusScan Enterprise now reliably reflects the status of On-Access Scans on the client system

7 **Issue** — McShield timed out after a DAT update. (Reference: 825043)

Resolution — Resolved a deadlock condition between the pause for update and trust validation.

8 **Issue** — On systems with large amounts of RAM and multiple cores, On-Demand Scans quit partially through scan activity. (Reference: 825623)

Resolution — Repaired a memory leak in the On-Demand Scan process. The read activity no longer increases memory

usage for entire scan.

9 **Issue** — The Help File provided with VirusScan Enterprise 8.8 Patch 2 was incorrect and did not include all languages. (Reference: 826008)

Resolution — This patch includes the correct help file with correct localization support.

10 **Issue** — On-Demand Scan exclusions were not properly excluded during scans. (Reference: 826029)

Resolution — Fixed the path comparison when the exclusion list includes items in a combination of file names with no extensions, path names, and wildcards.

11 **Issue** — The Outlook On-Demand scanner skipped scanning some items in PST files over 1GB when new mail activity was received. (Reference: 832626)

Resolution — The Outlook On-Demand Scan no longer counts incoming mail as part of storage scan.

12 **Issue** — If the system has multiple network adapters and Receive Side Scaling enabled, the server could accumulate an unlimited backlog of uncompleted UDP I/O, possibly exhausting memory. (Reference: 835879, 847944)

Resolution — Removed a bottleneck in the mfewfpk.sys driver that unnecessarily throttled network traffic.

13 **Issue** — In the ePolicy Orchestrator console, administrators reaching the text box limits for Access Protection policies: Rule Inclusions and Rule Exclusions fields were not warned before the limit was exceeded. (Reference: 835948)

Resolution — Increased text box sizes to allow over 5000 characters. In addition, ePolicy Orchestrator displays red warning text when fewer than 200 character spaces are available and again when fewer than 50 characters spaces are available.

14 **Issue** — Installation of VirusScan Enterprise 8.8 failed on some Windows XP and Windows 2003 systems. (Reference: 838476, 847143, 847220)

Resolution — Non-critical installation requirements were adjusted so that installation can proceed on these systems.

15 **Issue** — When multiple scan threads attempted to retrieve the virus list from DATs, the scanner threw an exception. (Reference: 851415, 848878, 850549)

Resolution — Scan threads retrieving the list of virus names are now protected from change by other threads.

16 **Issue** — When a file was excluded based on time, McShield threw an exception while processing ELAM reports. (Reference: 879062)

Resolution — Time-based On-Access Scan exclusions are no longer processed during ELAM validation.

17 **Issue** — On 64-bit systems, when opening the VirusScan Enterprise Console, an error sometimes occurred: `unable to connect to McAfee task manager service`. (Reference: 879062)

Resolution — Revised McAfee Task Manager to ensure process connections are available.

18 **Issue** — Bugcheck 24 occurred during the use of some virtualization products and included the Microsoft Filter Manager framework. (Reference: 889000, 906611)

Resolution — Fixed VirusScan Enterprise to ensure that I/O operations are always passed back to the Microsoft Filter Manager framework, when it is used.

19 **Issue** — A bugcheck could be caused when internal configuration data was being processed at the same time it was being updated. (Reference: 897517)

Resolution — Revised VirusScan Enterprise to ensure that configuration data is not modified while it is being processed.

20 **Issue** — In Metro mode, ScriptScan fails to load and execute. WWAHost.exe, which hosts and executes Metro Apps that use Java scripts, loads DLLs only from the system folder or apps package folder. ScriptScan resides in %program files%\systemcore folder. (Reference: 898855)

Resolution — Added proper access rights to ScriptScan so that WWAHost.exe can load it.

21 **Issue** — When matching file paths against Access Protection rules, the Access Protection driver could cause a system crash when the file path length is a certain size (including user-defined rules). (Reference: 757986)

Resolution — Improved string length tracking when performing rule matching operations.

22 **Issue** — A vulnerability allowed for unauthorized privilege escalation by an authenticated user. (Reference: 789945)

Resolution — This update resolves the vulnerability. Refer to online Security Bulletin SB10034 for the most current details.

23 **Issue** — McShield service remains in "Stop Pending" status. (Reference: 916102)

Resolution — Fixed thread synchronization issue related to update certificates thread and service main thread.

24 **Issue** — In certain environments, scheduled on-demand scans with credentials could fail due to an authentication failure even with correct credentials. (Reference: 778589)

Resolution — When authentication fails in these environments, Vsplugin now uses an alternative credential authentication method to launch the on-demand scan task successfully.

Issues resolved in Patch 3

These issues were resolved in the VirusScan Enterprise Patch 3 release.

1 **Issue** — On-Demand Scanner memory usage grows indefinitely when scanning large number of relatively small files. (Reference: 695931)

Resolution — The number of files in the scanner queue is now limited to 100, preventing the On-Demand Scanner memory from growing too large.

2 **Issue** — In an IPv6 environment, when a VirusScan Enterprise client sends an event with IPv6 information, the Threat Event log shows the IPv6 address as a string value instead of the original IPv6 address format. (Reference: 716512).

Resolution — The Threat Event log now correctly displays IPv6 addresses.

3 **Issue** — McAfee ePolicy Orchestrator queries using pie charts that group by VirusScan Enterprise version numbers display the client numbers accurately in the chart. However, when you drill down into one chart group, the filter is not applied and both workstations and servers are displayed. (Reference: 739627)

Resolution — VirusScan Enterprise 8.8.0 Patch 3 and later clients now report a new Machine Type property that classifies the client systems as Workstation or Server. Use this property in queries to filter against workstations or servers.

4 **Issue** — In specific situations, users could stop the McShield service. (Reference: 756805)

Resolution — Only administrative users can stop the McShield service.

Issues resolved in Patch 2

These issues were resolved in the VirusScan Enterprise Patch 2 release.

Patch

1 **Issue** — Third-party products that inject DLLs into processes could cause the VirusScan Enterprise service (VsTskMgr.exe) to periodically poll data and frequently log event 516 entries. (Reference: 625756)

Resolution — The VirusScan Enterprise Task Manager service no longer causes prolific generation of the event 516.

2 **Issue** — When a VirusScan Enterprise patch update is applied, the update would "succeed" and appear to be at the correct patch level even if a file was missing or corrupted in the repository. (Reference: 629564)

Resolution — A missing or corrupt patch file in the repository now causes VirusScan Enterprise updates to fail.

Note You must still manually fix the issue with the repository before the update can be successful.

3 **Issue** — A flaw in the Windows registry filtering model caused the McAfee Access Protection driver to incorrectly block remote registry accesses. (Reference: 668312)

Resolution — Microsoft identified a workaround and McAfee implemented the fix.

4 **Issue** — The Reports Extension might fail to check into the repository if the default group for the queries already exist. (Reference: 670759)

Resolution — All queries now include a group reference so they do not try to recreate the default group.

5 **Issue** — A STOP error (Bugcheck 7f) could occur with the McAfee filter driver due to lost content header information when transmitting through a raw socket on Windows 7. This issue was seen with some third-party VPN clients. (Reference: 682177)

Resolution — The McAfee filter driver now ensures header information is preserved and forwarded through a raw socket.

6 **Issue** — McShield might fail to start due to an API not properly calling processor group affinity for Non-Uniform Memory Access systems. (Reference: 685950)

Resolution — The API to set processor group affinity is now called correctly.

7 **Issue** — When a McAfee driver queried for the engine version, the return value was a non-empty string if a version was not found in the registry. (Reference: 689986)

Resolution — The return value has been updated to send an empty string if no engine version is found.

8 **Issue** — During an On-Demand Scan, the user was able to stop or cancel the scan, regardless of configured settings, by clicking the scan task in the console and selecting Show Progress. (Reference: 694042)

Resolution — Managed ePolicy Orchestrator On-Demand Scan tasks now properly enforce the password protection settings for the user if managed tasks are displayed in the user console.

9 **Issue** — Access Protection rules that begin with the special wildcard character "?", even with no rules set to block, would cause the CPU to spike to 100% usage. (Reference: 696654)

Resolution — The Access Protection driver now properly addresses the issue when evaluating rules beginning with "?".

10 **Issue** — A STOP error (Bugcheck 8E) could occur with VirusScan Enterprise if a locked file was being scanned under some circumstances. (Reference: 702469)

Resolution — VirusScan Enterprise now prevents the STOP error when scanning locked files.

11 **Issue** — When adding or removing a storage media device, the CPU usage could spike due to repeated attempts to acquire a resource that might be in an unguarded dead-lock state. (Reference: 703065)

Resolution — VirusScan Enterprise now recompiles rules from a separate thread to resolve the underlying dead-lock condition.

12 **Issue** — The Lotus Notes scan driver did not support the new multi-threaded Lotus Notes Client version 8.0 and later. (Reference: 708485)

Resolution — The Lotus Notes scan driver code now allows processing in multi-threaded Lotus Notes Clients version 8.0 and later.

13 **Issue** — The Lotus Notes scan driver sometimes encountered an out-of-bounds situation that caused an access violation, resulting in a crash on exit. (Reference: 712419)

Resolution — The Lotus Notes scan driver now handles the access violation, preventing a crash on exit.

14 **Issue** — If event ID 560 (security failure audit messages) was enabled, the event was logged during every policy enforcement. (Reference: 716044)

Resolution — Policy enforcement no longer causes Event ID 560 to occur on the client.

15 **Issue** — A STOP error (Bugcheck D5 or C2) could occur due to a race condition caused by a pool corruption with VirusScan Enterprise and Host Data Protection. (Reference: 726019)

Resolution — VirusScan Enterprise was modified to eliminate the pool corruption that could cause the race condition.

16 **Issue** — When an On-Demand Scan started, the wrong API call returned the machine name and user name individually and then concatenated them. (Reference: 726909)

Resolution — VirusScan Enterprise now calls the correct API to return the name of the user or other security principal associated with the calling thread.

17 **Issue** — When using Microsoft Outlook 2010 mail client, an On-Demand Email Scan would stop scanning mail items that returned a NULL session object. The VirusScan Enterprise Outlook Email Scanner was unable to scan NULL session objects. (Reference: 727314)

Resolution — The VirusScan Enterprise Outlook Email Scanner now skips scanning any NULL session objects.

18 **Issue** — Under low memory conditions, a STOP error (Bugcheck 8E) could occur due to failure with allocated memory from the system pool. (Reference: 727788)

Resolution — VirusScan Enterprise no longer causes a STOP error due to a memory allocation failure.

19 **Issue** — Some core files could fail to upgrade with VirusScan Enterprise 8.8.0 causing the installer to remove the core files from the system instead of reverting back to the previous state.(Reference: 730735)

Resolution — The installer now ensures the core files will not be removed from the system after a failed upgrade.

20 **Issue** — Some event XML data included empty strings, which are not honored by the event parser. (Reference: 732299)

Resolution — Empty strings are now accepted for the following fields in the XML events:

- FileName and VirusType for Detection events
- ProcessName for PortBlock events

21 **Issue** — ScriptScan URL exclusions did not allow several special characters, including '/', in the ePolicy Orchestrator VirusScan Enterprise policy settings. (Reference: 733717)

Resolution — ScriptScan URL exclusions with now will not allow only '*' and '?' as originally intended.

22 **Issue** — A STOP error (Bugcheck 7E) occurs due to a race condition between internal interface registration and deregistration. (Reference: 735108)

Resolution — Simplified internal synchronization to avoid a registration race condition.

23 **Issue** — A STOP error (Bugcheck D5 or C2) would occur from a race condition caused by corruption in the kernel pool when attempting to free a buffer that had already been freed. (Reference: 735511)

Resolution — VirusScan Enterprise was modified to eliminate the race condition that could corrupt the kernel pool.

24 **Issue** — When installing to a machine with Host Intrusion Prevention, Host Intrusion Prevention blocks a McAfee process (mfehidin.exe) from setting Access Control List (ACL) on a McAfee driver (mfevtps). (Reference: 735512)

Resolution — The Host Intrusion Prevention Entercept Agent service is now stopped before upgrading the syscore drivers and vscore files.

25 **Issue** — Lotus Notes Scanner does not support the new multi-threaded environment of Lotus Notes Clients version 8.0 and later. (Reference: 740019)

Resolution — Lotus Notes Scanner is now thread-safe in multithreaded environments of Lotus Notes Clients version 8.0 and later.

26 **Issue** — Access Protection would cause incompatibilities with some Microsoft Windows component installers. (Reference: 740244)

Resolution — Access Protection was modified to remove the incompatibility.

27 **Issue** — Attempting a remote connection to the SAP server using the WebIRichClient with On-Access Scanner enabled prevented the system from connecting and caused the WebIRichClient software to become non-responsive. (Reference: 741714)

Resolution — The file filter was revised to temporarily delay a scan if a file had been modified under conditions that could block concurrent access through the file system.

28 **Issue** — The McAfee McShield service could encounter a dead-lock situation in an internal utility routine when processing scans of modified files. In this case, the McShield internal dead-lock watchdog timer fires and the McShield service stops. (Reference: 754042)

Resolution — Scans of modified files are now conducted with corrected context information passed to internal utility routines, avoiding the dead-lock situation.

29 **Issue** — When running an On-Demand scan on disk volumes where Update Sequence Number (USN) journals are not enabled, the last access time of the corresponding files might be updated. (Reference: 756797)

Resolution — VirusScan Enterprise On-Demand scanner no longer modifies the file time stamp while performing scans.

30 **Issue** — If a file was cached as clean and then later added to the User Defined Detections (UDD) in the Registry, the file is not detected by the On-Access Scanner until the service restarts. (Reference: 762155)

Resolution — On-Access Scanner resets the cache so when the file is added to UDD it will now be detected.

31 **Issue** — STOP error (Bugcheck 50) could occur as part of handling changes to the Windows PendingRename registry value by referencing an invalid memory location. (Reference: 773909)

Resolution — VirusScan Enterprise no longer accesses invalid memory locations when processing the PendingRename registry value.

Repost Patch

1 **Issue** — The uninstall scripts do not detect the latest version of AV Kaspersky 6.0.4 when installing VirusScan Enterprise. (Reference: 701815)

Resolution — When installing VirusScan Enterprise, the uninstall scripts now detects and removes AV Kaspersky 6.0.4.

2 **Issue** — The REBOOT=A option to SetupVSE.exe did not reboot the system if launched from a scheduled task. (Reference: 717989)

Resolution — SetupVSE.exe now enforces the REBOOT=A option, even if the user is not logged on interactively.

3 **Issue** — When upgrading from VirusScan Enterprise 8.5.0 to VirusScan Enterprise 8.8.0, an outdated driver was left installed. In some instances, the old driver remained loaded in memory. (Reference: 741085)

Resolution — The installer now removes the outdated driver. A system reboot might be required to remove the driver from memory and load the correct driver. The installer does not force a reboot.

Issues resolved in Patch 1

These issues were resolved in the VirusScan Enterprise Patch 1 release.

Patch

1 **Issue** — Installation fails with ERROR 1920, citing The McShield Service failed to start. This can occur when Microsoft Windows is installed to a sub-folder rather than the root. (Reference: 638858)

Resolution — The system core installer has been revised to recognize all system paths.

2 **Issue** — A Bugcheck 5 error could occur if memory allocations are not checked for failure, resulting in an invalid memory reference. (Reference: 643013, 651019, 673463, 676448)

Resolution — The memory allocation is now checked for success prior to referencing it.

3 **Issue** — Malicious software might change NTFS folder permissions on McAfee folders in order to disable the software. (Reference: 643440)

Resolution — Self protection now protects McAfee folders, files and registry data from permission changes.

4 **Issue** — Process exclusion for Buffer Overflow was broken after introducing more granularity in Buffer Overflow exclusions using Module Name and API Name. (Reference: 651569, 686711, 687670)

Resolution — Process exclusions for Buffer Overflow work as expected on standalone machines, ePolicy Orchestrator managed systems and during ePolicy Orchestrator Policy Migration.

5 **Issue** — When multiple signatures are included in an EXTRA.DAT, the buffer used to store the description information for the "About" window might not be large enough. (Reference: 651670)

Resolution — Buffer size for storing Extra.DAT signature information has been increased to 4 times its original size.

6 **Issue** — When the option “Show add-in user interface error” is enabled in Outlook, the following pop-up error appears every time Outlook is started and the first e-mail is opened or created: “Custom UI Runtime Error in McAfee E-mail Scan Add-in”. (Reference: 651887, 656365, 656366, 656644, 656674, 656678, 657131, 657398, 657409, 657411, 657413, 657414, 657433, 661628, 675246)

Resolution — McAfee E-mail Scan Add-in has been fixed to return correct “success” error code to Outlook. The pop-up error no longer appears.

7 **Issue** — Files on network locations might trigger an unhandled exception leading to a system crash if the network experiences a failure or the object is unreadable. One report of this occurred when opening Outlook 2010 with PST files

configured to reside on remote storage. (Reference: 660014, 663389, 665822, 667934)

Resolution — The exception is handled to avoid a system crash.

8 **Issue** — Access Protection rules involving the block of System:Remote fail to enforce. This also applies to preventing remote access to shares. (Reference: 661424)

Resolution — VirusScan Enterprise identifies remote share access and enforces Access Protection rules that prevent remote access to shares.

9 **Issue** — The XML file generated for Event 1202 contained incorrect values for GMTTime and UTCTime fields. (Reference: 661702, 676893)

Resolution — GMTTime and UTCTime fields for Event 1202 now have the correct time information.

10 **Issue** — TA Bugcheck C2, “Bad_Pool_Caller” error, could occur under varied conditions. One instance was triggered when using Virtual Machine Converter. (Reference: 662350, 666697, 673448, 678179, 690657, 691258)

Resolution — A memory corruption issue has been resolved.

11 **Issue** — A variety of symptoms, including an application crash, might occur with the ScriptScan feature disabled. (Reference: 662684, 665748, 668796, 668807, 669035, 669605, 669773, 669875, 671666, 671668, 671671, 671672, 672710, 675259, 675261, 676492, 685467, 685551, 685566, 685650, 686667, 686828, 687336, 693321, 696789, 696834)

Resolution — ScriptScan DLLs are no longer accessed if the feature is disabled.

12 **Issue** — An attempt to add an exclusion to the Access Protection rule "Protect Internet Explorer favorites and settings" failed when the edit box reached its maximum limit. (Reference: 663135)

Resolution — Buffer size for storing processes to exclude has been increased, enabling customers to add exclusions.

13 **Issue** — When filtering network Input/Output, a timing issue could occur, leading to a kernel thread stack exhaustion. This issue could result in a system crash. (Reference: 664539, 665345)

Resolution — VirusScan Enterprise now uses a Deferred Procedure Call to ensure a fresh thread stack.

14 **Issue** — A bugcheck 50 error could occur when a McAfee driver encountered unexpected data while examining loaded resources of a third-party application. (Reference: 667172)

Resolution — The McAfee driver has been updated to handle this situation.

15 **Issue** — A memory leak could occur with the process validation service and the Microsoft .NET runtime support library, mscoree.dll. (Reference: 673462)

Resolution — Changes made to the process validation service have removed the dependency of the Microsoft .NET runtime support library, mscoree.dll.

16 **Issue** — When Hotfix 660014, which introduces folder permission restrictions, is installed, McAfee Agent installations might be blocked by an Access Protection rule. (Reference: 684965, 686259, 686272)

Resolution — The McAfee Agent is no longer blocked when trying to set folder permissions.

17 **Issue** — A defect in the matching engine prevents the deletion of folder names that are a substring of “Program Files”, such as “c:\pro” or “c:\prog”. (Reference: 685273)

Resolution — The matching engine now only matches complete folder names, so deleting “Program Files” is prevented, but deleting “C:\pro”, “c:\prog”, or other substrings is allowed.

18 **Issue** — An issue in the clean-file scan cache logic was identified on systems supporting the Server Message Block 2 (SMB2) protocol that could allow files to be written to a share and not be scanned. (Reference: 686645, 686650, 690277)

Resolution — When On-Access Scanner tries to scan a share file and the scan does not succeed, the scanner now returns an OPLOCK error to McShield. McShield returns NOTSCANNED status to the driver and the file is not added to the cache, causing the file to be scanned when accessed.

19 **Issue** — When Hotfix 660014, which introduces Access Protection rule: Prevent modification of McAfee files and settings, is installed, VirusScan Enterprise prevents installation and adding features to Windows systems. (Reference: 691269, 691651)

Resolution — VSCAN.BOF content file has been modified to properly restrict access to McAfee files and settings.

20 **Issue** — The On-Demand Scanner cleanup events (1034, 1035, 1202, and 1203) have timestamps that are identical to the On-Demand Scanner start time. (Reference: 691660)

Resolution — VirusScan Enterprise now obtains the current time before generating On-Demand Scan cleanup events.

Repost Patch

1 **Issue** — When installing VirusScan Enterprise, the installer checks for the existence of UNC paths in the PATH environment variable. If found, VirusScan Enterprise will block the installation because of an issue with McShield. (Reference: 657079, 657651)

Resolution — SetupVSE.exe now includes a bypass flag that allows the installation to continue on machines with UNC paths in their PATH environment variable.

2 **Issue** — When upgrading from VirusScan Enterprise 8.7i to VirusScan Enterprise 8.8, the Access Protection rules from an older version (8.7) of the product were used. (Reference: 659049)

Resolution — The installation now loads the correct Access Protection rule-set.

3 **Issue** — When upgrading from VirusScan Enterprise 8.7i (without the McAfee AntiSpyware Enterprise module) to VirusScan Enterprise 8.8, the McAfee AntiSpyware scanner did not have the default detections defined. (Reference: 663995)

Resolution — The installer now detects that McAfee AntiSpyware Enterprise is being installed for the first time and now sets the default scanning options.

Installation instructions

Use these instructions to install, verify, and remove this VirusScan Enterprise Patch release.

Requirements

This Patch release works with the following VirusScan Enterprise releases.

<table>
<tr><th>Package</th><th>VirusScan Enterprise version</th><th>Notes</th></tr>
<tr><td>Patch 4</td><td>VirusScan Enterprise 8.8.0 Patch 1</td><td rowspan="3">Important This package does not upgrade VirusScan Enterprise version 8.8.0.777 (RTW).

To install this package on VirusScan Enterprise 8.8.0:
• On 64-bit systems, first install Patch 2, then Patch 4.
• On 32-bit systems, first install Patch 1, then Patch 4.</td></tr>
<tr><td></td><td>VirusScan Enterprise 8.8.0 Patch 2</td></tr>
<tr><td></td><td>VirusScan Enterprise 8.8.0 Patch 3</td></tr>
</table>

		Alternatively, uninstall VirusScan Enterprise 8.8.0 and reinstall with the **Repost Patch 4** package.
Repost Patch 4	New system installations	
	VirusScan Enterprise 8.7i systems	

Minimum versions

This release supports the following minimum versions.

- **Scan Engine**: 5600
- **Detection Definitions (DAT)**: 7000+
- **McAfee Agent:**
  - 4.8.0.641
  - 4.6.0.2288
  - 4.5.0.1810

Install the product

Install this patch directly to a target client system or use ePolicy Orchestrator to deploy this release to managed systems.

Client	ePolicy Orchestrator
To install this patch directly to a target client system: 1 Extract the patch files to a temporary folder on your hard drive. 2 Double-click the setup file in the temporary folder created in Step 1: • Patch: Double-click Setup.exe. • Repost Patch: Double-click SetupVSE.Exe. 3 Follow the installation wizard instructions. **Note** You might need to reboot the system to fully load the system drivers into memory however, the package installation does not force the reboot.	To deploy this release to managed systems: 1 In the ePolicy Orchestrator Master Repository, check in the VirusScan Enterprise zip package. Select the Product or Update (.ZIP) package type. 2 If this release includes VirusScan Enterprise reports or extension files, extract them from the package zip file and check them into the ePolicy Orchestrator repository separately. 3 Deploy to the client systems: • Patch — Use a McAfee Agent Product Update client task. • Repost — Use a McAfee Agent Product Deployment client task.
For more information, see the *VirusScan Enterprise Installation Guide*.	For more information, see *Checking in packages manually* in the ePolicy Orchestrator online help.

Verify the client installation

After installing VirusScan Enterprise Patch 4, verify that the product installed correctly.

Before you begin

Reboot the client system prior to validating that the installation is successfully installed.

Task

- Check any of the following items:
  - After the ePolicy Orchestrator agent collects property information, the client system details display the HotFix/Patch version.
  - On the client system, check for a registry key entry Patch_4 in HKey_Local_Machine\Software\McAfee\DesktopProtection.

    Note On a 64-bit system, this entry might be located in HKey_Local_Machine\Software\Wow6432Node\McAfee\DesktopProtection.

  - Confirm that the expected files are installed by checking the version number of individual files. File versions should match the list of files in *File inventory* section.

Note Releases are not displayed or do not report installed if an error occurred during installation, or if a file did not install correctly.

File inventory

File name	Version (x64/x86)	File name	Version (x64/x86)	File name	Version (x64/x86)
mfevtps.exe	15.1.0.656	adslokuu.dll	15.1.0.543	BBCpl.dll	8.8.0.1247
mfeapconfig.dll	15.1.0.656	csscan.exe	15.1.0.543	condl.dll	8.8.0.1247
mfeapfa.dll	15.1.0.656	dainstall.exe	15.1.0.543	consl.dll	8.8.0.1247
mfeapfk.sys	15.1.0.656	entvutil.exe	15.1.0.543	graphics.dll	8.8.0.1247
mfeavfa.dll	15.1.0.656	ftl.dll	15.1.0.543	mapprem.dll	8.8.0.1247
mfeavfk.sys	15.1.0.656	lockdown.dll	15.1.0.543	mmalnot.dll	8.8.0.1247
mfebopa.dll	15.1.0.656	mcshield.dll	15.1.0.543	naiann.dll	8.8.0.1247
mfebopk.sys	15.1.0.656	mcshield.exe	15.1.0.543	NCDaemon.exe	8.8.0.1247
mfeclnk.sys	15.1.0.656	mcvssnmp.dll	15.1.0.543	NCExtMgr.dll	8.8.0.1247
mfeelam.dll	15.1.0.656	mfeann.exe	15.1.0.543	NCInstall.exe	8.8.0.1247
mfeelamk.sys	15.1.0.656	MfeOtlkAddin.dll	15.1.0.543	NCMenu.dll	8.8.0.1247
mfehida.dll	15.1.0.656	mytilus3.dll	15.1.0.543	NCScan.dll	8.8.0.1247
mfehidin.exe	15.1.0.656	mytilus3_server.dll	15.1.0.543	NCTrace.dll	8.8.0.1247
mfehidk.sys	15.1.0.656	mytilus3_worker.dll	15.1.0.543	odspause.dll	8.8.0.1247
mfehidk_messages.dll	15.1.0.656	naevent.dll	15.1.0.543	shcfg32.exe	8.8.0.1247
mferkda.dll	15.1.0.656	naievent.dll	15.1.0.543	shstat.dll	8.8.0.1247

mferkdet.sys	15.1.0.656	OtlkScan.dll	15.1.0.543	shstat.exe	8.8.0.1247
mfetdi2k.sys	15.1.0.656	OtlkUI.xxx.dll	15.1.0.543	shutil.dll	8.8.0.1247
mfevtpa.dll	15.1.0.656	scriptff.dll	15.1.0.543	vsodscpl.dll	8.8.0.1247
mfewfpk.sys	15.1.0.656	scriptsn.xxx.dll	15.1.0.543	vsplugin.dll	8.8.0.1247
mscan32.dll	5.600.0.1067	RkScan.dll	1.0.0.231	VsTskMgr.exe	8.8.0.1247
Mscan64a.dll	5.600.0.1067	VSCAN.BOF	659	wscavexe.exe	8.8.0.1247
				wscav.dll	8.8.0.1247

Remove installation files

Remove the patch installation files using Add/Remove Programs.

For information on removing the VirusScan Enterprise product, see the *VirusScan Enterprise Installation Guide*.

Important Removing the patch from a client system places the client system in an unsupported state. See *Known issues* for further details.

Task

1. To remove the patch manually, use Add/Remove Programs. (You must have administrative rights to the local system.)

   All features affected by the patch are reset to installation defaults. Any features not modified by the patch are left with their current settings.
2. Update VirusScan Enterprise after removing the patch to ensure that VirusScan Enterprise is running the latest version of the engine and DAT files.

Known issues

For a list of known issues in this product release, see this McAfee KnowledgeBase article: KB78495.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1. Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.
2. Under Self Service, access the type of information you need:

To access...	Do this...
User documentation	1 Click Product Documentation. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click Search the KnowledgeBase for answers to your product questions. • Click Browse the KnowledgeBase for articles listed by product and version.